F-Secure Mobile Security for Android Ver.15

ユーザーズガイド

20150713-152

目次

第 1 章：インストール....4
インストール....5
認証....5
F-Secure Mobile Securityを設定する....6
F-Secure Mobile SecurityをAndroidデバイスからアンインストールする....6

第 2 章：データの保護をする....7
リモートアンチセフトを有効にする....8
リモートロック....8
リモート削除....8
リモートロケート....9
SMS警告....9
アンチセフトのアラームを使用する....9

第 3 章：ブラウザ保護....10
ブラウザ保護を有効にする....11
ブラウザ保護を使用する....11
インターネットを安全に利用する....11

第 4 章：ウイルスをスキャンする....12
マニュアル スキャン....13
感染したファイルの処理....13
スケジュールスキャンを設定する....13

第 5 章：お子様/未成年に安全なインターネット環境を設定する....14
許可するコンテンツを指定する....15
許可するアプリケーションを指定する....16

第 6 章：特定の電話番号からの着信とメールを拒否する....17
連絡先フィルタ....18
ブロックした着信とメッセージを確認する....18

第 7 章 : プライバシー侵害 19
アプリのプライバシー 20

第 8 章 : F-Secure Mobile Securityを更新する 21
更新モードを選択する 22
手動更新 22

第
1
章

インストール

トピック ：

・*インストール*
・*認証*
・*F-Secure Mobile Securityを設定する*
・*F-Secure Mobile SecurityをAndroidデバイスからアンインストールする*

ここでは、F-Secure Mobile Securityをモバイルのデバイスにインストールするための方法を説明します。

F-Secure Mobile Securityのインストール後、ライセンスを認証してください。ライセンスを認証したら、デバイスは保護されます。

インストール

Mobile Securityをモバイルデバイスにインストールする方法について説明します。

Mobile Securityを旧バージョンからアップグレードする場合、旧バージョンをアンインストールする必要はありません。アップグレード後、Mobile Securityの設定が正しく継承されていることを確認してください。

Mobile Securityをインストールするには

1. Google PlayからデバイスへMobile Securityをインストールします。
2. インストール後、[開く] を選択して、正規ライセンスキーを認証し、製品版に移行します。

認証

ライセンスを認証すると、製品版になります。

ライセンスを認証するには

1. F-Secure Mobile Securityを起動します。

   利用規約が表示されます。
2. 内容を確認し、同意する場合、[OK] を選択します。
3. 最初に「評価版」でインストールを完了します。

   その後、詳細 > ライセンスの順に選択します。

   「キーコードをお持ちですか？」をクリックし、製品版ライセンスキーコードを入力します。
4. [認証] を選択します。

   👉 注:　認証中にMobile Securityはエフセキュアの更新サービスに接続します。

認証後、製品の機能を設定します。

なお、アンチセフトを利用するためにデバイス管理者を有効にする必要があります。

F-Secure Mobile Securityを設定する

F-Secure Mobile Securityを使用する前に製品の設定を行う必要があります。

次の方法でアンチセフト、ペアレンタルコントロール、コールブロッカーを有効にできます。

1. セキュリティコードを作成します。

   👉 注: セキュリティコードを後で変更するには、アンチセフト（またはペアレンタルコントロール）> 設定を開き、[セキュリティコードを変更する] を選択します。

   アンチセフトのリモート機能とペアレンタルコントロールを利用するにはセキュリティコードが必要となります。

2. デバイスの管理を行うための認証を行います。デバイス管理者を有効にするために [有効にする] を選択します。

3. デバイスのスクリーンロックを設定していない場合、スクリーンロックを設定します。

   詳細については、デバイスの取扱説明書を参照してください。

4. メールアドレスを入力します。

   セキュリティコードを忘れたときにこのメールアドレスにリセット案内が送信されます。

5. 信頼済みの電話番号を入力します。

   デバイスのSIMカードが変更されたときに信頼済みの電話番号に通知が送信されます。

アンチセフトを設定したらステータス：デバイスは保護されています に表示が変わります。

F-Secure Mobile SecurityをAndroidデバイスからアンインストールする

デバイスからF-Secure Mobile Securityをアンインストールする方法について説明します。

F-Secure Mobile Securityをアンインストールするには

1. メインビューで [詳細] を選択します。
2. [アンインストール] を選択します。

   アンチセフトのセキュリティコードを作成した場合、アンインストールを行うためにセキュリティコードを入力する必要があります。

F-Secure Mobile Securityがデバイスから削除されます。

👉 注: 「デバイス管理者」の一覧で本製品が無効になります。アンインストールをキャンセルすると、製品をもう一度認証する必要があります。

第
2
章

データの保護をする

トピック ：

- *リモートアンチセフトを有効にする*
- *SMS 警告*
- *位置情報を共有するアンチセフトのアラームを使用*

アンチセフトを使用すると、デバイスを紛失した場合でもデバイスの本体とデータを保護することができます。

デバイスを紛失しても、デバイスに SMS を送ることでデバイスをロックすることが可能です

・一度デバイスをロックすると、アンロックパターンを利用しない限り、デバイスのロックを解除することはできません。

注: 「リモートロック」を使用するには、デバイスのアンロックパターンを有効にする必要があります。

・一度デバイスをロックすると、セキュリティコードを利用しない限り、デバイスのロックを解除することはできません。

「リモート削除」は、デバイスのデータをリモートで削除する機能です。

・デバイスにリモート削除を指定する SMS を送ると、デバイスのデータ（SD カード、SMS/MMS メッセージ、連絡先、カレンダーの各データ）が削除されます。リモート削除を行う場合、セキュリティのために Google アカウントのパスワードを変更することを推奨します。

・リモート削除の SMS をデバイスに送るときにデバイスの全設定が初期化されます。

WiFi のみのタブレットには、アンチセフトは、ありません。

リモートアンチセフトを有効にする

リモートアンチセフトを有効にすると、デバイスにSMSを送ることでデバイスのロックまたはデータの削除を行うことが可能になります。

リモートアンチセフト設定するには

1. メインビューで［アンチセフト］を選択します。
2. 「アンチセフト」メニューから［有効］を選択します。
3. スクリーンロックを設定します。
4. セキュリティコードを設定します。
5. 「メールアドレス」を入力します。これは後でも設定可能です。
6. 「信頼済みの番号（携帯電話）」を入力します。これは後でも設定可能です。

アンチセフトが有効になります。

リモートロック

「リモートロック」は、デバイスをリモートからロックして、第三者がデバイスを使用することを阻止します。

デバイスをリモートからロックするには

1. 次の内容のSMSを別のデバイスからこのデバイスに送ることでこのデバイスをロックできます。
   #LOCK#<セキュリティコード>（例: #LOCK#12345678）
2. リモート削除を行うと、SMSを送信したデバイスへ返信メッセージが送られます（一部の機種のみ）。

一度デバイスをロックすると、このデバイスのスクリーンロック設定を変更しない限り、デバイスのロックを解除することはできません。

リモート削除

「リモート削除」は、デバイスのデータをリモートから削除して、第三者がデバイスのデータを使用することを阻止します。

リモートからデバイスのデータを削除するには

1. 次の内容のSMSを別のデバイスから送ることでデバイスのデータを削除できます。
   #WIPE#<セキュリティコード>（例: #WIPE#12345678）
2. リモート削除を行うと、SMSを送信したデバイスへ返信メッセージが送られます。（一部の機種のみ）

リモート削除を行うと、SD カード、SMS/MMSメッセージ、連絡先、カレンダーの各データが削除されます。また、リモート削除のSMSをデバイスに送るときにデバイスの全設定が初期化されます。

リモートロケート

デバイスを見失った場合、デバイスにSMSを送ることでデバイスの位置を検索することが可能です。

👉 注: デバイスの位置情報を検索するには、デバイスのGPS機能が有効になっていること、スクリーンロックが有効である必要があります。

デバイスの位置を検索するには

次の内容のSMSを別のデバイスからデバイスに送ることでデバイスの位置を検索できます。

#LOCATE#<セキュリティコード>（例: #LOCATE#12345678）

しばらくしてからデバイスの位置を知らせるSMSが届きます。

👉 ヒント: 本製品をデバイスにはじめて設定するときには、リモートロケート機能の動作を確認するためにロケート用のSMSを検証用に送ることを推奨します。

👉 注: アンチセフトはSMSを通じてデバイスの位置データを送りますが、そのデータを保存することはありません。

SMS警告

アンチセフトは、デバイスのSIMカードが変更された場合にSMSを別のデバイスに送る「SMS警告」機能を搭載しています。

SMS警告を有効にするには

1. メインビューで［アンチセフト］を選択します。
2. 「アンチセフト」メニューから［設定］を選択します。
3. ［信頼済みの番号］を選択します。
   「信頼済みの番号」を設定する画面が開きます。
4. SIMカード変更時に送るSMSの送信先（電話番号）を指定します。

SMS警告が有効になります。

アンチセフトのアラームを使用する

デバイスの紛失や盗難時にアラーム（警告音）を鳴らすことができます。

アラームを設定するには

1. 次の内容のSMSを別のデバイスからデバイスに送ることでアラームを再生できます。
   #ALARM#<セキュリティコード>#<再生回数>（例: #ALARM#12345678#3）
   👉 注: 再生回数でアラームを鳴らす回数を指定できます（指定しなくてもアラームは鳴ります）。
2. SMSを受信すると、デバイスがロックされ、アラームが鳴ります。SMSを送信したデバイスへ返信メッセージが送られます（一部の機種のみ）。

設定したスクリーンロックを利用することでアラームを無効にできます。

👉 ヒント:次の内容のSMSを別のデバイスからデバイスに送ることでアラームをリモートから停止する事もできます。#ALARM#<セキュリティコード>#0

第
3
章

ブラウザ保護

トピック：

- ブラウザ保護を使用する
- インターネットを安全に利用する

ここでは、ブラウザ保護（セーフブラウジング）の機能について説明します。ブラウザ保護は個人情報（クレジットカード情報、ユーザアカウント情報、パスワードなど）を盗むWebサイトからユーザを保護します。

ブラウザ保護を有効にする

ブラウザ保護を設定するには

1. メインビューで［セーフブラウジング］を選択します。
2. ［有効］を選択します。

ブラウザ保護を有効にすると、保護されているブラウザが一覧で表示されます。そして、ブラウザ使用時に、危険なWebサイトがブロックされるようになります。［戻る］を選択すると、前の画面に戻れます。
ブロックしたWebページで表示される[Webページにアクセスする］リンクをクリックすると、ブロックしたページにアクセスすることが可能です。

ブラウザ保護を使用する

本製品の専用ブラウザ(セーフブラウザ)に加え、ブラウザ保護は、組み込みブラウザ、Chome、Dolphinに対応しています。
ブラウザ保護を有効にした状態で、本製品を実行している限り、ブラウザ保護は継続的に有効になります。
ブラウザ保護は透過的に動作し、ブラウザ使用時にユーザがアクセスするWebサイトを自動的にチェックします。つまり、対応ブラウザの利用時にブラウザ保護を使用します。
ただし、ペアレンタルコントロールを有効にした場合、保護されているブラウザはモバイルセキュリティのSafe Browserのみになり、セーフブラウジングを無効にすることができません。
ーブラウザ保護（セーフブラウジング）を利用する前にブラウザのキャッシュをクリアして下さい。

インターネットを安全に利用する

ブラウザ保護を使用すると、危険性のあるWebサイトにアクセスすることを防ぐことができます。
Webページにアクセスする際にWebページの安全性が自動的に確認されます。アクセスしようとしているWebページが「不審」または「危険」と評価されている場合、Webページのアクセスがブロックされます。
Webページの評価は、エフセキュアのマルウェア分析やパートナーからの調査などに基づいています。

第
4
章

ウイルスをスキャンする

トピック：

- マニュアル スキャン
- 感染したファイルの処理
- スケジュール スキャン

F-Secure Mobile Securityはデバイスに対してウイルスと悪質なコンテンツのスキャンを行います。

F-Secure Mobile Securityは、インストール済みのプログラムおよびデバイスに装着されているメモリーカードに対してウイルス、スパイウェア、リスクウェアのスキャンを行います。

👉 注： F-Secure Mobile Securityがデバイスをスキャンするよう警告を表示したときにはスキャンを実行することを推奨します。

マニュアル スキャン

必要に応じて、手動でウイルスのスキャンを実行することができます。

手動でスキャンを実行するには

1. メインビューで［アンチウィルス］を選択します。
2. ［スキャンする］を選択します。

   ウイルススキャンが開始します。
3. スキャンが完了したら、次の情報が表示されます。

   ･感染 － 検出された感染の数を示します。

   ･不要な可能性のあるアプリ－ 長い間使用されていないアプリの数
4. ［OK］を選択してスキャンを終了します。

感染したアプリケーションやファイルが検出されたら、デバイスから削除することを推奨します。

感染したファイルの処理

特定のファイルに感染が検出された場合、感染したファイルをデバイスから削除することができます。

感染したファイルを処理するには

1. メインビューで［アンチウィルス］を選択します。
2. ［感染したファイル］を選択します。

   感染したファイルの一覧が表示されます。
3. 処理するファイルを選択します。
4. 感染したファイルを選択すると、ファイルの詳細を確認できます。「感染の詳細」画面では、感染したファイルのパスと名前、および感染の原因となるウイルス名が表示されます。
5. ［削除］または［アンインストール］を選択すると、感染したファイル/アプリケーションを取り除きます。

ウイルス、トロイの木馬、ワーム、その他のマルウェアに関する追加/詳細情報は、エフセキュアのWebサイト（*http://www.f-secure.com/virus-info/*）でご覧になれます。

スケジュールスキャンを設定する

定期的にスキャンするようにスケジュールが設定できます。

スケジュールスキャンを設定するには

1. メインビューで［アンチウィルス］を選択します。
2. ［設定］を選択します。
3. 「スケジュールスキャンを有効にする」にチェックを入れスキャン間隔・スキャン時間を設定します。

第
5
章

お子様/未成年に安全なインターネット環境を設定する

トピック：

- 許可するコンテンツを指定する
- アプリケーション通信制御を使用する。

ペアレンタルコントロールはお子様/未成年がインターネット上の望ましくないコンテンツにアクセスすることを阻止します。また特定のアプリケーションの１日の使用時間を制限することが可能です。
インターネットには数多くの面白いWebサイトがある反面、お子様や未成年に危険性があるのも事実です。お子様/未成年のユーザはモバイルデバイスを利用してインターネットにアクセスすることが一般的になっており、ほとんどの場合その行動は監視されていません。多くのWebサイトにはお子様や未成年に対して望ましくないコンテンツが含まれているため、お子様/未成年がそのようなコンテンツさらされてしまうことは簡単です。また、ウイルスなどの不正なファイルを誤ってダウンロードしたり、嫌がらせのメールを配信されたりすることも可能です。
ペアレンタルコントロールを利用することで、お子様/未成年のユーザが不正なコンテンツにアクセスすることを制限できます。

許可したコンテンツ/コンテンツタイプ

ペアレンタルコントロールを使用して、コンテンツ別にWebサイトのアクセスをブロックすることができます。ペアレンタルコントロールのWebサイトのアクセス制限はデフォルトのSafeBrowser（セーフブラウザ）を利用することで機能します。
またペアレンタルコントロール有効時は、組込みブラウザ、Chrome、Dolphinを起動した場合でもセーフブラウザが起動します。

- アダルト
  性的な表現や性描写を含む成人向けのコンテンツを示します。アダルトショップやヌードなどの性的コンテンツ。
- チャット
  Webベースのチャットプログラムやインスタントメッセージ用ソフト、チャットサイトなど。
- Webメール
  メールアカウントを作成できるサイトやブラウザを通じてメールを送受信できるサイトなど。
- 武器
  武器の写真や説明、爆弾の作り方を含むサイトなど。
- ギャンブル
  オンラインカジノ、ギャンブル関連のWebサイトなど。
- 麻薬
  薬物使用を促すサイト。麻薬の栽培や売買に関する情報を含むサイトなど。
- 出会い系
  出会い系やメールオーダーブライドのサイトなど。
- ソーシャルネットワーク
  プライベートやビジネスの交流に関する社会的ネットワークを提供するサイトなど。
- 掲示板
  コメントを表示/投稿できるオンライングループや掲示板を作成できるプログラムなど。
- ブログ
  オンラインの日記や個人Webページ、ブログ、ポッドキャストなど。
- ショッピングとオークション
  Web上で商品を直接注文できるサイトや価格比較、インターネットのオークションサイトなど。
- カルト
  宗教、その他のイデオロギーに反対する熱狂的なグループを支援するサイトなど。
- お酒とタバコ
  お酒やタバコに関する製品の情報を提供、促進、支援するサイトなど。
- 憎悪表現と暴力
  特定の宗教、人種、民族、性別、年齢層、障害者、性的指向に対する差別を示すサイト、または暴力、動物虐待、機関への破壊行為に関する写真や説明を含むサイトなど。
- 違法ダウンロード
  プログラムの違法/不審なアクセスを提供するサイト、またはネットワークやシステムに問題を発生させるプログラムを開発および配布するサイトなど。
- アノニマイザー
  インターネットの行動を追跡できないようにするサイトやフィルタを回避する情報を提供するサイトなど。
- 不明
  コンテンツが認識されないサイトは、「不明」のカテゴリとして指定されます。

許可したコンテンツ/アプリケーション

ペアレンタルコントロールを使用して、アプリケーションの制限とアンインストールを行うことができます。

許可するアプリケーションを設定するには、

1. メインビューで［ペアレンタルコントロール］を選択します。
2. ペアレンタルコントロール 有効（on）の状態で、［許可したコンテンツ/アプリ］で、インストールされているアプリケーションの一覧が表示されます。
3. アプリケーションの使用を許可する場合、アプリケーションの横にあるチェックボックスをオンにしてください。チェックボックスをオフにすると、アプリケーションが制限されます。デフォルトではペアレンタルコントロールは全アプリケーションのアクセスを許可します。

制限したアプリケーションを起動しようとすると、アプリケーションがブロックされていることを示すページが表示され、アプリケーションのアクセスがブロックされます。

第
6
章

特定の電話番号からの着信とメールを拒否する

トピック：

- 連絡先フイルタ
- ﾌﾞﾛｯｸした着信とﾒｯｾｰｼﾞを確認

連絡先フィルタ（コールブロッカー）を有効にすると、特定の電話番号からの着信とSMS/MMS メッセージを拒否することができます。
連絡先フィルタを使用して、望ましくない電話や迷惑メッセージをブロックできます。
着信とSMS/MMS メッセージのブロック対象となる電話番号を指定することができます。ブロックした電話番号に電話をかけることも禁止されます。
WiFiのみのタブレットには、コールブロッカーは、ありません。

連絡先フィルタ（コールブロッカー）

連絡先フィルタは、特定の電話番号からの着信とメッセージを拒否する機能です。

特定の電話番号からの着信とメッセージを拒否するには

1. メインビューで［コールブロッカー］>［設定］を選択します。
2. ［ブロックリスト］を選択します。

   セキュリティコードを設定します(設定していない場合)。
3. ブロック対象の電話番号を入力します。
4. ［保存］を選択して、指定の電話番号をブロック対象に設定します。

連絡先フィルタを有効にすると、ブロックされている電話番号からの着信とSMS/MMSメッセージが拒否され、発信も禁止されます。

ブロックした着信とメッセージを確認する

連絡先フィルタのブロック履歴で拒否した着信とメッセージを確認することができます。

連絡先フィルタのブロック履歴を表示するには

1. メインビューで［コールブロッカー］>［設定］を選択します。
2. ［ブロック履歴］を選択します。
3. 拒否した電話番号等が表示されます。

第
7
章

プライバシー侵害

トピック：

- アプリのプライバシー

インストールされているアプリケーションで、プライバシー問題の可能性があるものをランク別に表示します。

アプリのプライバシー

インストールされているアプリケーションで、プライバシー問題の可能性があるものをランク別に表示します。

1. メインビューで［アプリプライバシー］を選択します。

   ランク別にアプリの数を表示します。

2. ［アプリケーションを表示］を選択します。

   問題のアプリケーション名を表示します。

3. 表示しているアプリケーション名を選択すると具体的な問題点を確認することができます。

4. 選択したアプリケーションを削除（アンインストール）することができます。

第
8
章

F-Secure Mobile Securityを更新する

トピック：

- 更新モードを選択する
- 手動更新

F-Secure Mobile Securityの「自動更新」機能は、ウイルスの定義ファイルやプログラム本体を自動的に更新する機能です。
F-Secure Mobile Securityを認証した時点で自動更新が有効になります。自動更新はインターネットに接続している際に更新を確認し、更新がある場合には更新をダウンロードします。

👉 注: F-Secure Mobile Securityの自動更新機能は有効なライセンスを必要とします。

更新モードを選択する

F-Secure Mobile Securityをインストールしたら自動更新が有効になります。自動更新またはリアルタイムスキャンを無効にした場合、更新を手動で行う必要があります。

更新モードを選択するには

自動更新のモードを選択します。

- マイプロバイダ – デバイスがホームネットワークに接続している場合、更新を自動的にダウンロードします。
- 全プロバイダ – 更新を定期的にダウンロードして、ウイルス定義ファイルを最新の状態にします。
- 無効 – ウイルス定義ファイルを自動的に更新しないようにします。自動更新を無効にすることは推奨しません。

手動更新

Mobile Securityを手動で更新することもできます。

更新を手動で確認するには

1. メインメニューで［詳細］>［更新］を選択します。
   更新を確認するにはインターネットの接続が必要です。
2. ［更新］を選択します。
   新しい更新が利用できる場合、ダウンロードの確認が表示されます。
3. ［はい］を選択して、更新をダウンロードします。
4. ダウンロードが完了したら、［インストール］を選択します。